SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology

Singh, Saurabh; Ra, In-Ho; Meng, Weizhi; Kaur, Maninder; Cho, Gi Hwan

Published in:
International Journal of Distributed Sensor Networks

Link to article, DOI:
10.1177/1550147719844159

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Advances in Cyber Physical Social Systems (CPSS) - Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2019, Vol. 15(4)

DOI: 10.1177/1550147719844159
journals.sagepub.com/home/dsn
SAGE

SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology

Saurabh Singh[1], In-Ho Ra[2], Weizhi Meng[3], Maninder Kaur[4] and Gi Hwan Cho[1]

Abstract

The growing demand for human-independent comfortable lifestyle has emboldened the development of smart home. A typical keenly intellective home includes many Internet of things contrivances that engender processes and immensely colossal data to efficiently handle its users' demands. This incrementing demand raises a plethora of concern cognate to a smart home system in terms of scalability, efficiency, and security. All these issues are tedious to manage, and the existing studies lack the granularity for surmounting them. Considering such a requisite of security and efficiency as a quandary at hand, this article presents a secure and efficient smart home architecture, which incorporates the blockchain and the cloud computing technologies for a cumulated solution. Because of the decentralized nature of blockchain technology, it can serve the processing services and make the transaction copy of the collected sensible user data from smart home. To ensure the security of smart home network, our proposed model utilizes the multivariate correlation analysis technique to analyze the network traffic and identify the correlation between traffic features. We have evaluated the performance of our proposed architecture using different parameters like throughput and discovered that blockchain is an efficient security solution for the future Internet of things network.

Keywords

Internet of things, cloud computing, blockchain, security attacks

Date received: 20 August 2018; accepted: 19 March 2019

Handling Editor: Shancang Li

Introduction

The amelioration of the Internet of things (IoT) in the day-to-day life is able to connect an immensely colossal number of smart devices such as sensors, cameras, phones, and many smart home appliances. Radio frequency and sensor network innovations have incentivized many IoT applications to build smart homes in the recent years. Smart home applications integrate the smartness into a residence in order to make a situation for occupants comfortable and safety.[1] R Lutolf defines the concept of smart home in his research article. According to him, the smart home is an integration of

[1]Division of Computer Science and Engineering, Chonbuk National University, Jeonju, South Korea
[2]School of Computer, Information and Communication Engineering, Kunsan National University, Gunsan, South Korea
[3]Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby, Denmark
[4]Computer Science & Engineering Department, Thapar Institute of Engineering and Technology, Patiala, India

Corresponding author:
Gi Hwan Cho, Division of Computer Science and Engineering, Chonbuk National University, Jeonju 54896, South Korea.
Email: ghcho@chonbuk.ac.kr

various services within home by using a common communication system. It also guarantees the economical, comfortable services and security with a high degree of flexibility and smart functionality.[2] The smart home-cognate technology with various kind of algorithms used with paramount in smart home since past, future, and present time. Considering this, the keenly intellective domicile can be tenacious as a domain that consists of a highly accustomed application where users merge all the incipient concepts and technologies. This automation has the feature of intelligent devices and appliances that use wired as well as wireless technologies and software to facilitate seamless integration of home system.[2,3]

Although in the early stages, IoT and smart expectations are increasingly being transactional in homes across the country. The Gardener research report forecast that the IoT contrivances will be incremented by a maximum of 24 billion IoT-enabled devices, and Industrial Development Corporation (IDC) project will grow by $1.7 trillion in economical IoT market.[4] Due to an enormous increase in these smart devices, the traditional methods of handling network like server-client communications are profoundly cumbersome.[5] Moreover, like Cyber Physical Social Systems (CPSS), many applications share physical world entities in the social systems. Many of them have interdependency problems. The CPSS are relatively complex system and have ranged to multiple complexes and various devices, to highly heterogeneous networks. Cyber Physical Systems (CPS) domains include manufacturing, smart healthcare, smart grids, smart homes, smart cities, and transportation.[6]

Furthermore, threats and attacks on the network communication system produce many challenges regarding security and privacy for the keenly intellective home. Pishva and Takeda[7] reviewed and discussed security threats in smart homes.[8] The authors discussed variants of attacks and obviation methodologies. Depending on the appliance type and attack category, the authors presented a summarized threat-likelihood level that categorizes the attack potential. As the security is on top of the list of consumer demands, the approaches must consider scalability and availability for efficiently monitoring and managing the network which needs dynamic adoption capabilities for IoT environment.[9]

To inhibit these issues and to achieve the trust and integrity, an innovative exploration of blockchain technology and cloud computing for the distributed IoT predicated smart home environment is presented in this article. The distributed nature of blockchain makes it brilliant to handle security for independently operating entities in a smart home. Blockchain has an immutable public record of data which is secured by peer-to-peer participants. With the magnification of the 5G network and edge devices, the blockchain sanctions more expeditious and efficient communication without any single point of failure.[9,10] Because of decentralization nature of blockchain technology, it ascertains scalability and robustness utilizing resources of participating nodes and eliminates the many-to-one traffic. It also diminishes delay to overcome the single-point failure.

Over the year, cloud computing has offered services through dynamically scalable and resource virtualization mechanisms. It reveals a significant potential to provide on-demand computing service to the consumers with high flexibility, scalability, and availability. In addition to these mechanisms, a multivariate correlation analysis (MCA) detection technique is used to analyze the smart home network traffic flow which helps to classify the correlation between the traffic features.

Security and privacy concerns in smart home are rapidly growing in IoT networks. In Jacobsson and Davidsson,[11] authors mentioned many researches toward a model of privacy and security for smart homes. With the increasing of smart devices entering into the market raises the concern of security and privacy in the IoT network. The integration platform solution of large enterprises in technology has spread. Amazon will leverage its smart home platform to deliver home-made food directly to the refrigerator. But security is a concern for the customer's home where the contractor can be robbed. In addition, future passwords may be leaked out or your home may be hacked. It is what a big player needs to plan.

Enterprise and homeowner data sharing is perhaps the next generation of data distribution services in smart home technology. For example, to order the food it requires to maintain the refrigerator's temperature for delivery purpose. Sharing of data with smart device is of great interest to enterprises that manufacture these products. It increases efficiency. Technology is efficient enough to control the wireless volume, security, and security appliance.

Distributed blockchain technology is useful for interoperating new use cases emerging in the diagnosis of home appliances, energy saving, and prevention of major damage in case of natural disaster.

Concerns, challenges, and lack of technology that is introduced in smart home network are motives for providing a security architecture. Introducing blockchain and MCA algorithm into the smart home will lead to an effective innovation for security surveillance system to combat crime, as many people are willing to work from their home to protect their physical and intellectual property. The need for reliable, scalable, manageable, secure, and energy-efficient smart home environment is a motivation for conducting research in smart home while exploring issues and challenges and providing a solution. Based on the challenges and the requirements of network technology which is applied in

an IoT environment, the article contributions are as follows:

- The article proposes an IoT smart home architecture based on cloud computing and blockchain technology.
- The article explains the blockchain technology applied in a smart home network for handling the device transactions and uses green cloud computing, which provides green service using a green broker to reduce the environmental effects of the proposed model.
- A security analysis algorithm is presented by using MCA algorithm for detection of denial-of-service (DoS)/ distributed denial-of-service (DDoS) attack in the smart home network.
- The experimental analysis is performed in a smart home network by using parameters like memory utilization, network delay, and network overhead with detailed results for execution time and throughput.

The structure of the article is as follows: The "Related work" section describes related work on blockchain technology, green cloud computing, challenges in IoT smart home and smart home services. The proposed IoT based smart home architecture and security analysis are explained in the "Proposed architecture" section. The "Experimental analysis" section illustrates the performance evaluation of proposed architecture. Finally, The "Conclusions" section concludes the article.

Related work

This part discusses the details of the existing solutions as well as technologies used in this article.

Distributed blockchain

A blockchain is a technique that allows all members to maintain a containment ledger of all transaction data and to update the ledger when there are new transactions to maintain consistency. Blockchain is truly a mechanism that grants everyone high accountability with no missed transaction. It guarantees the validity of transaction by maintaining a register on the node that validates the transaction but also distributes that register to the entire network. With the advancements of the Internet and its encryption technology, it becomes possible for all members to verify the responsibilities of transactions, so that dependency on authorized third parties is resolved and a single point of failure is removed.[12]

There are some obvious advantages to the idea of building a smart machine that can communicate and operate over a blockchain.

When data transactions occur across multiple networks owned and managed by multiple organizations, permanent records mean that they can be tracked as data. Blockchained records are inherently transparent. All activity can be tracked and analyzed by anyone with network connectivity. In addition, the "smart contract" functionality provided by some blockchain networks, such as Ethereum, allows you to create contracts that run when conditions are met. Blockchain and IoT are promising technologies to keep. Both are already widely and enthusiastically adopted in the industry and public sector. One of the most interesting aspects of blockchain technology is that data are not stored in one central point but are completely decentralized. This eliminates the need for a strong central authority and gives the control back to the individual user. Furthermore, for supply chain management, blockchain technology offers the benefits of traceability and cost-effectiveness. It is used to track the movement of goods, origin, quantity, and so on. This brings a new level of transparency to the B2B ecosystem.

To ensure that only legitimate transactions are added to the blockchain, the network verifies that the new transaction is valid and also prevent from invalidation of the previous transaction. A new data block is added to the blockchain only after the computer on the network has reached an agreement on the validity of the transaction. The consensus in the network is due to other voting mechanisms and the most common one is a proof of work that depends on the amount of processing power donated to the network. Once a block is added to the ledger, the block can be permanently placed to it, and transactions contained in the block can be accessed and verified by all users on the network.[13]

The blockchain is the structured list which stores data in a similar format as a distributed database. It is designed to be easily manipulated as the participants in the networks store and verify blockchain. Each block in the ledger has a header and body as shown in Figure 1. The header contains the hash value of the current block and previous block, a nonce, and a timestamp. The body part consists of transactions. Index method is used to retrieve the block data.

Green cloud computing

The researchers for the cloud computing are considering the unique advantage of empowering the computing system. Cloud computing provides the pay-per-use type of service to eliminate upfront investments. The basic five components of cloud computing that help to build an efficient smart home are virtualization, multitenancy, cloud storage, hypervisor, and cloud

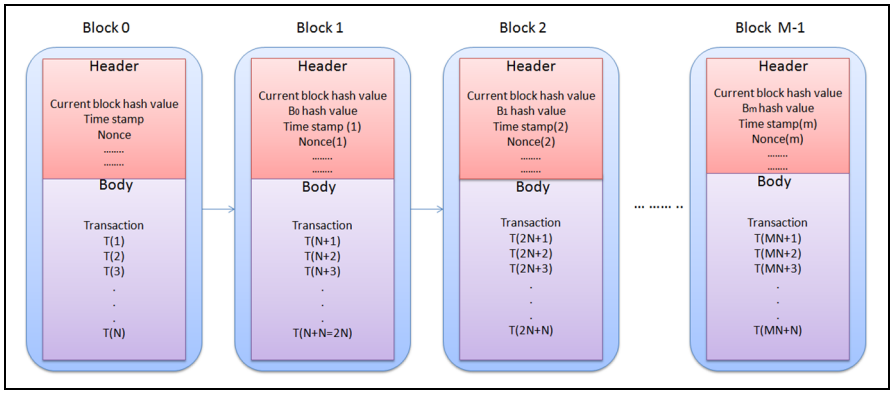

Figure 1. An exemplary illustration of the structure of blockchain.

network.[14] It must satisfy the service-level agreement (SLA) with the wide variety of requirements by third-party organizations to reach the quality of service. As for a smart home is concerned, all the information will be received from the nodes and send to the cloud via a smart gateway.

For a cloud infrastructure, energy consumption and carbon emissions are important concerns. The key driver technology in an energy-efficient cloud is the process of presenting a logical group or piece of computing resources. Cloud computing also offers facilities for green computing by delivering flexible, geographically distributed, cost-effective, and energy-aware services. There are many approaches related to virtualization in order to eliminate the energy inefficiency problem and get lower carbon emissions. As per the existing studies, the carbon emission can be reduced to 30% per user by migrating application in the cloud.[15,16]

Many other approaches also propose an optimization cost model to calculate the cost of service and also ideas of minimizing the power consumption. Several factors are taken into consideration for calculating the energy consumption such as single task as a unit, related analysis tool, empirical method, and different runtime task as well as scheduling of workload.[17,18]

IoT smart home challenges

Security and privacy: Communication of real-life objects creates huge challenges in trust, security, and privacy. IoT has already been facing many security threats and attacks. Due to enormous data transmissions, the communication of important data in the network might be attacked by some adversaries such as the man-in-the-middle (MitM) attack and DoS/DDoS attack. IoT causes many unique challenges to privacy such as data privacy issues and tracking devices for phones and cars. In addition, voice recognition is being integrated to listen to conversation for actively transmitting data to cloud storage for processing.

Scalability and access control: Since IoT supports a huge number of devices which connect and communicate with each other, scalability is considered to be one of the major challenges faced by the middleware approach. Hence, a reliable middleware is required to manage the number of devices which effectively handle the scalability issues in order to function well in a small and large IoT environment.[19] Access control permits users to access resources of IoT system. Due to an increase in the number of devices as well as resource demand, and low bandwidth between devices and Internet, the system faces access control challenges. In addition, because of unbounded number of resources and subjects access control mechanism should be extensible in structure, size, and users.

Availability and reliability: Dynamic and adaptive functionalities are required to manage and monitor the IoT infrastructure in a self-manageable mode. This will allow a permanent solution to availability and reliability for the dynamic and robust connection. The IoT availability is explained by many researchers as closely related to reliability requirement. The IoT system not only needs to guarantee a certain level of performance required by the application but also needs to exhibit sufficient elasticity to maintain availability at the desired level.

Confidentiality and integrity: Confidentiality is the protection of information especially when shared in the public network. It ensures users' privacy and kept safe the user private information. Confidentiality requires an efficient cryptography and key management in order to achieve high anonymity. In spite of several solutions, still, there are attacks against confidentiality that expose routing information and exchange data.[20] Integrity ensures that there is no modification of data in a smart home environment that faces issues of integrity problem. An attacker can modify sensed data that are to be stored in node or while it travels in the network.[21]

Smart home services

Smart home involves a service provided at home that enables residents to live more conveniently, comfortably, and smoothly. Each subsystem is a kind of people's goal for intelligent households and corresponds to a smart home-centric Cloud service.[22]

Environmental: Mainly centralized controllers are associated with HVAC, water, auto-tuning, and adaptive or remote controllable lighting, which can make your everyday life convenient and efficient and save energy. Typical case: When one goes outside, devices such as air conditioners, lights, gas, and other unwanted household appliances operate in standby mode or turn off to conserve energy and protect the home.

Security: If the motion and environmental detectors detect abnormal home conditions (e.g. fuel/smoke, leaks, window breakage, or trapped in the bathroom), an alarm is generated and delivered to the homeowner over the phone, the Internet, or via turning on the surveillance camera. One can trigger a series of service requests and responses after connecting to a vulnerable zone or a corresponding service. Every member who enters or leaves your home triggers the relevant solution (identity authentication, auto-lock).

Domestic appliances: Proposal and introduction of the online recipe, automatic cooking and cleaning, smart refrigerator with stock check, and so on.

Information and communication: Information from the smart home is delivered to telephone and PC via Internet using a security alarm and a home calendar, and the relationship between the smart home system and another service provider is established.

Health: The health monitor maintains vigilance at the moment "when you are indoors" and periodically measures vital sign parameters and gathers information in patient's records.

Security and privacy issues in CPSS

Because of more complex systems and heterogeneous network, CPSS are more susceptible to the targeted attacks. CPSS include cyberspace, physical space, and social space. Malicious users can attack CPSS from multiple link sources, such as GPS in social space or location data coming from a user's handheld device or user authentication information in cyberspace. If reasonable security and privacy mechanisms are missing, a malicious attacker may eavesdrop on that sensitive information.[23]

Indeed, security vulnerabilities have been found in more and more cyber physical systems, such as electronic grid, smart transport system, and medical system. Because of these vulnerabilities, many attacks occur that results in a big concern on security and privacy in terms of integrity, availability, authenticity in CPSS. Some attacks are as follows.[24]

Eavesdropping: CPS are particularly vulnerable to be eavesdropped through traffic analysis, likewise intercepting monitoring data transferred in the sensor network collected through monitoring process. Privacy is also compromised by eavesdropping attack such as patient's personal health status data transferred to the system.

Compromised key attacks: In fact, an attacker can gain a key even if the process is difficult and resource intensive. For example, an attacker can capture a sensor to perform a reverse engineering task to determine the internal key. An attacker can impersonate a valid sensor node to deceive to match a key with another sensor.

MitM attack: In CPS, authenticity is aimed at realizing authentication in all related processes like sensing, communication, and operations. In an MitM attack, a fake message is sent to the operator and may take the form of false negatives or false positives. As a result, the operator can take actions such as turning over the breaker when it is not necessary, or when it is necessary to act, everything seems to be normal and action is not taken.

DoS attack: The CPS take place by embedding sensing, computation, and communication technologies in a physical system. After accessing the CPS network, an attacker can create the following situation:

- Flood the controller or the entire sensor network into traffic until an overload causes a shutdown.
- Incorrect shutdown or service behavior occurs if incorrect data are sent to the controller or system network.
- Block traffic to get loss of access to authorized elements in the system from accessing network resources.

MCA detection approach

MCA plays an important role in the field of data analysis based on feature extraction technique of original and legitimate data. This technique is characterized by extracting the geometric correlation between network traffic functions.[25] Complete detection process consists of three phases as shown in Figure 2.

Step 1: Initially, basic feature are generated from admission traffic in defined interval.
Step 2: MCA applied the triangle area generation module to separate the co relation between two particular features.
Step 3: Decision making of data based on training and testing phase.

Existing research

Houbing et al.[26] discussed the application area of CPS along with specific domain in cybersecurity and privacy. In Houbing et al.,[27] it is explored that CPS may

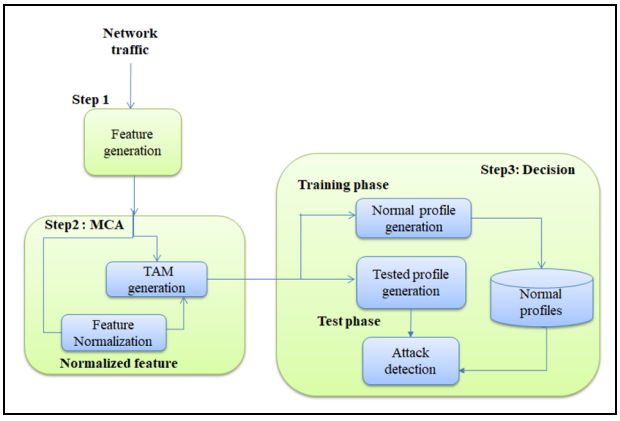

Figure 2. MCA detection approach.

help to improve the coordinated control, regulations, monitoring system in smart city, and supporting sustainability objects.

Amadeo et al.[28] proposed a framework for smart home service based on information centric network. A three-layered architecture consists of remote cloud, fog layer with smart home servers and end devices. The framework supports real-time services deploying smart monitoring and efficient control application.

Stojkoska and Trivodaliev[29] have reviewed challenges and solution for IoT smart home toward narrowing the gap between the existing state-of-the-art smart home applications and the prospect of their integration into an IoT-enabled environment. The author proposed a framework that incorporates components of existing IoT architecture. The article mentioned challenges of data processing and communication protocols.

Yunchuan et al.[30] promote the vision of Smart and Connected Communities (SCC). The vision is to improve preservation, livability, revitalization, attainability, and security of a community. The authors present TreSight, a case study that integrates IoT with cyber physical cloud computing and big data for smart tourism.

Proposed architecture

The proposed SH-BlockCC architecture will take the advantage of cloud computing and blockchain technology to achieve efficiency, scalability, and availability to make the smart home greener. The architecture contains four components, that is, smart home layer, blockchain network, cloud computing, and service layer as shown in Figure 3.

Smart home layer

Smart home represents a single family, intelligent households which consists of many IoT devices and other subsystems like security system, control system, home theater, and so on. These devices have sensors which communicate with each other through a centralized application. The sensor devices data are communicating with cloud and their services. The data from IoT network are received by cloud platform which also integrate with other device data. It also combined with business transaction data. Many smart home networks require home services by the efficient service providers.

Distributed blockchain layer

Blockchain has recently received attention from stakeholders in a variety of industries. The reason for this is that blockchain technology allows applications to be manipulated in a distributed fashion which previously used to run through a trusted intermediary. It is an openly distributed ledger which records multiple transactions in an effective and verifiable way without any master host in the entire chain. Similar practice can be utilized with the same service contract without a central authority. Blockchain technology provides a distributed peer-to-peer network in which untrusted individuals without trusted intermediaries can communicate empirically with each other.

Blockchain in distributed cloud storage. *Decentralized and trust*: Blockchain brings decentralized structure which has no single authority that approves the transaction. To ensure trust in blockchain, the nodes in the network have to reach the consensus to accept the transaction.

Complete privacy: In blockchain, each user maintains its own key. It stores encrypted fragments of user data using cryptocurrency system and has the potential to overcome various privacy issues.

Facilitate resource usage and high quality: It facilitates the resource usages by its distributed application. For example, a smart contract needs to execute resource-demanding algorithm by using some cryptographic functions. And that application provisions a computer on demand resource algorithm from smart contracts, by which the payment will happen automatically after function have been executed.

In summary, by using the blockchain quality of service can be improved by providing the traceability of resource usage in a way that both customer and provider can verify the SLA and also determine which party is responsible for the reported faults.

Transaction handling of blockchain in smart home. All the devices are managed by transactions and stored in the local blockchain. The transaction can be done by local device communication or between overlay nodes. Each transaction is programmed for some functions such as store and access, monitor, Mode of formation, and

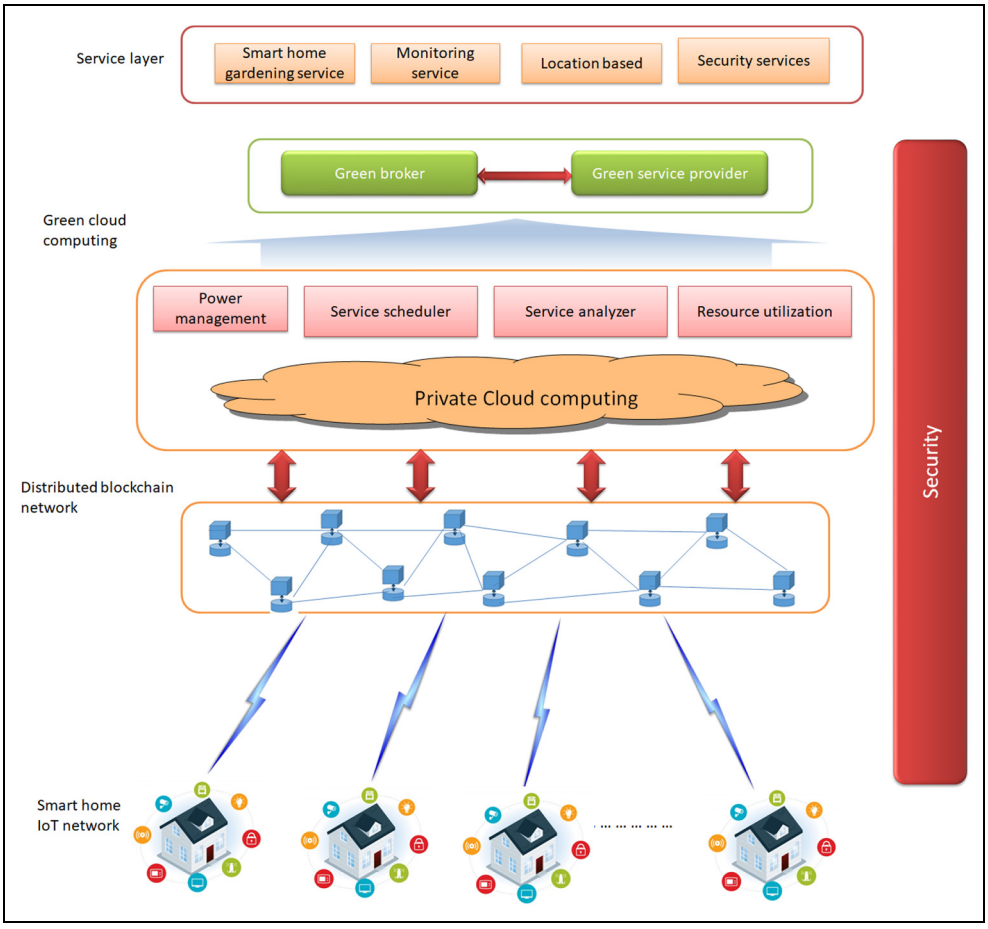

Figure 3. Proposed smart home architecture.

remove. A shared key is used by all the transaction generated by the Diffie-Hellman algorithm. In the smart home, to add any device the minor creates a genesis transaction which is designed to add a new device to a smart home by using a shared key. The lightly weighted hashing is to detect the variations in the transaction content. To get the user control over the transaction, a shared key is used to allocate to the device by the minors. And in order to allocate the key, the minors check the policy header and ask the permission from the owner and distribute the shared key. As a result, the device is able to communicate as long as the key is valid.

Adding a new device is done through the genesis process, whereas for accessing the data, two different methods are followed: the first one is local access and the second is access the cloud. For local access, the device sends a request to the miner to check the permission and take the data from local storage. For access to the cloud, a miner can request the data from cloud storage and send it back to the device.

The device can also demand to store the data on local storage as well as on cloud storage. The whole process is called store transaction. For locally storing the data, the device requires authentication to the local storage and send a request to miners to check that weather device has to store permission or not. If permission is allowed, the key is shared between the device and local storage and device can store the data directly to local storage. To store the data in the cloud, it requires identical blocks associated with the unique number. The block number and hash of the saved data are used by the user for authentication. After the successful authentication process, the data packets from the user are stored in the block along with hash in First-in-First-out (FIFO) order. Therefore, the service provider can access the data and provide smart services efficiently.

In summary, the smart home consists of a number of different types of IoT devices connected to each other through a network. The devices are managed by the local blockchain. As the smart home IoT devices are resource-constrained devices, symmetric key encryption is used for the local transaction. The block manager is responsible for managing the blockchain. It manages the generation, verification, and storages of individuals

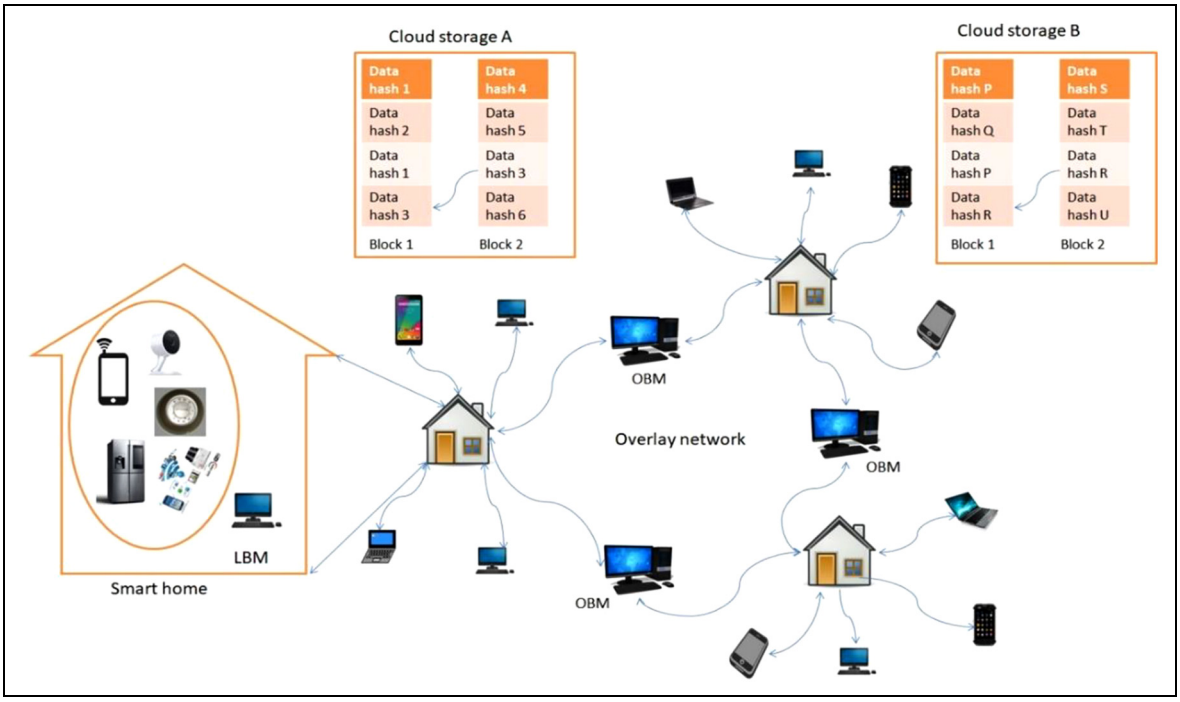

Figure 4. An overview of overlay network connecting smart home, OBM, and cloud storage.

as well as blocks of the transaction. Every smart home maintains a local ledger which processes all local and overlay transactions of the smart home. The Diffie-Hellman algorithm is used for key exchange between two entities.

Overlay network. An overlay network is a computer network which consists of a large number of nodes connected by virtual links. It is built on the top of another network. Since overlay network consists of many nodes (which maintain the scalability and decreases overhead), cluster head of each cluster is selected by using a clustering algorithm as discussed in Abbasi and Younis.[31] The whole network is managed by public blockchain. As a result, the cluster head is also known as Overlay Block Managers (OBM) as shown in Figure 4. Overlay BCs are maintained on all CHs in the overlay network, including multiple signed transactions sent by cloud storage and access transactions. Unlike Bitcoin mining, each CH independently determines whether to retain or discard a new block based on communication with the received transaction partner. This could lead to different versions of BC for each CH.

Transaction in the overlay network is done by requester node which generates the transaction and requester which is transaction receiver. This is called overlay transaction and it uses asymmetric encryption, digital signature, and digital hash function. The whole network relies on public key infrastructure (PKI) system and each node maintains its public key. Certificate Authority (CA) approves the node's public key with the signed certificate. To initiate any transaction, the node creates genesis transaction which includes certificate which is verified by OBM. Overlay transactions are broadcast and verified by the OBMs. Overlay network act as a peer-to-peer network to get anonymity at internet protocol (IP) layer.[32] An OBM verifies a transaction by validating the signature of the transaction participants with their public key. All the valid transactions are stored in a predefine block. In addition, the OBM verifies if the previous transaction of each transaction, which is stored in the previous transaction field, exists in the public BC. Each OBM maintains a list of three things: (a) public key of requester that can access smart home data attached to this cluster, (b) public key of requester which is a list of smart home public keys connected to the cluster where access is permitted, and (c) a list of transaction that forward to other OBM.

Access transaction for IoT device. To provide a decentralized access of IoT data, a requester joins a consortium blockchain network which is a decentralized peer-to-peer network and runs its own blockchain. It is responsible for securing logging of incoming request of user's IoT data and performing access control to those requests. Therefore, requester joins consortium network via client application, that is, the user can make the request data. Now, for IoT data sharing, the local blockchain manager of smart home adds the requester public key to its smart contract. The local blockchain or private blockchain is also known as sidechains. The sidechain network generally forms with grouping the

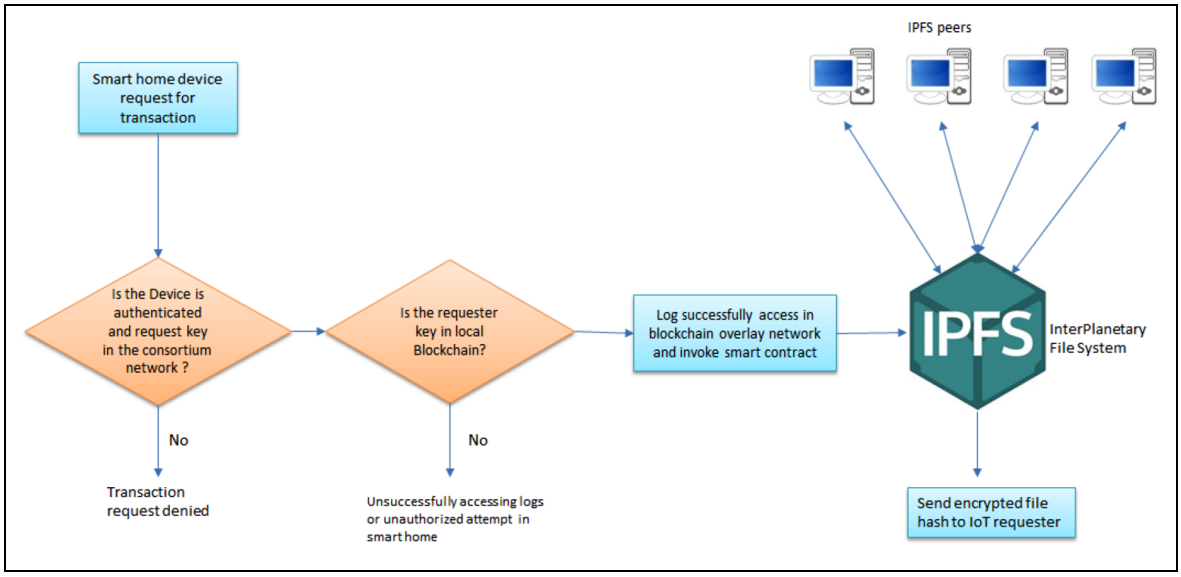

Figure 5. Methodology for access request transaction of IoT device.

IoT devices used for any singular use case. User can own its own sidechain networks and each are responsible for maintaining secure log IoT data operations within the network. One more benefits of making sidechain is that the IoT devices participating in one sidechain's consensus algorithm, there is no need to validate transactions occurs in other different sidechains. Now, after adding the public key of requester to the sidechain of smart contract have gotten the access privilege. At this moment, the validator node which has higher computational power, storage space and have IoT device's unique public and private key, added the same requester's public key to the list of authorized requester in the consortium network.

To access the users' IoT data, the requester signs the access request transaction using his private key and follows the flow chart of step taken in response to an incoming access request on the consortium network as shown in Figure 5. After receiving encrypted InterPlanetary File System (IPFS) hash file, the requester can decrypt it with its private key. Therefore, it ensures the privacy of data and no alteration of data within the network. A wise agreement on the consortium blockchain also prevents the requester from flooding the consortium blockchain with illegal request transactions. If the requester makes a specified number of consecutive failure requests, the smart contract removes the associated public key from the list of approved supplicants.

Cloud layer

Green broker and CSP. To make the cloud service more energy efficient, green broker plays an important role in selecting the service provider for the users. Broker manages the client request more in a more environmentally friendly manner while dealing with all the three main services of SaaS, PaaS, and IaaS. Each broker has a public directory which has a record of service cost value, carbon emission, access time, and other information. It also has job scheduler, job selector, carbon emissions calculator. Generally, the three elements that are included while offering green cloud are the following:

- Third party: It has carbon emission directory listing their cloud service and respected energy efficiency.
- Users: Selecting most green cloud providers
- Providers: Enabling the most carbon efficient operation of clouds

In this way, enterprises can reduce the carbon footprint by at least 30% per user by migrating applications to the cloud.

Multi-tenancy and data center efficiency. The new service model that leverages virtualization and remote access in cloud computing has expanded the implications of multi-tenancy architecture. For example, a SaaS provider can run one instance of an application on one database instance and provides web access to different customers. In this case, data are isolated for each tenant without visibility to others. Multi-tenancy can be cost-effective because it shares software development and maintenance costs.

As far as the efficiency of the data center in the cloud is concerned, it mostly impacts the energy consumption of cloud computing. The efficient technology used in the data center will improve the power usage efficiency

and realizes several benefits such as managing redundancy in multiple servers in multiple locations. Cloud computing allows accessing and interchange services among the data centers by using virtualized services, monitoring an account.

Cloud topological structure. It is same structure as typical cloud structure on a smart home. The difference comes through by adding the smart home as a kind of infrastructure and integrating middleware into cloud platform to make the smart home resource available. At the gateway, smart home acts like a single virtualized node. The nodes that belong to the cluster are components of smart home cloud and are parts of cloud architecture distinguished only by the types of service to be provided. Home gateway controls all the services and makes them available to the devices outside of the home. Connecting the smart home automation to clouds, it aims to build the intelligence space which interconnects the home appliances and links to the service provided by the clouds. It also allowed the third parties to create and deploy their own appliances. It also searches for external resources and notifies home appliances how to use them.

Green cloud computing. *Power management*: the model aims to efficiently maintain the power management of the data center. It focuses on resource efficiency that reduces servers' power consumption or data center space. That means with less equipment plugged in, data center will consume less energy.

Service scheduler: Considering of many smart home connected and build smart building and city, it assigns requests to VMs and determines the resource entitlements to allocate the VMs. It also decides to add or remove VMs as per demand.

Service analyzer: This interprets and analyzes the submitted requests before deciding whether to accept or reject the Smart Home's service requirements. As a result, smart home needs the latest load and energy information through the VM Manager and the green broker on the Energy Monitor, respectively.

Resource analyzer: It manages the availability of smart home services to end users in the efficient way. It manages the resources to improve the cloud computing performance by reducing energy consumption, e-waste, as well as using heterogeneous and geographically distributed resource to meet smart home clients' request.

Smart home oriented cloud. It considers the smart home that merges into a cloud to get more information from the cloud and services. The cloud is not based on the current cloud architecture, but it extends its service offerings to provide special and efficient home services for digital consumer electronics. The three basic elements which enable home automation become easy and fit for future demands. (a) The infrastructure part that consists of many physical and virtual resources designed for cloud service delivery which is managed by large computing power, storage, and network resources. (b) The platform consists of resource and the security management module. Resource module manages the system process detection and implements resource virtualization. And security management module protects the cloud security, including reliability and authentication, data investigation, and reconfiguration. A PaaS-based cloud can provide service providers with a platform to deploy tailored services to smart home consumers. (c) The service layer interacts with the service providers and smart home users. Its focuses on application service through application program interface (API) interface provided by the cloud platform. Users use services or applications provided by smart home clouds, enterprise public clouds, or other third-party clouds.

Security analysis of DoS/DDoS attack in the smart home

This section presents the analysis of smart home network based on anomalies in the traffic. The anomaly detection algorithms presented in this section detects and acts against the DoS/DDoS attack. The goal is to test the smart home experience with IoT devices and to initiate internal and external attacks on IoT devices to validate our approach. Algorithm 1 and algorithm 2 are service providers for the client and detection and

Algorithm 1. Security approach for smart home network

```
Start
state←Service provide
  while (t_l∈T has not expired) do
    if (client c_i is authenticated == "Yes") then
      if (query q_i is matched == "Yes") then
        if (q_i is identified as old packet query == "No") then
          Process for the response to c_i
        else if
          Detection and mitigation as in Algorithm 2
          Update database
        end
      else
          Response to c_i that the q_i is not valid
      end
    else
      Deny the query
      Update database
    end
  end
end
```

Algorithm 2. Anomaly detection and mitigation

```
Start
state←Detection and mitigation
while (t2∈T has not expired) do
    Arrive a new query qi
    if (qi == "Yes") then
        Check the signature si of qi with known attack
        if (si == True) then
            Discard the qi
        else
            Extract the feature of the qi for the traffic using
            TAM of MCA
            Check the anomaly pattern pi of qi
            if (pi == True) then
                Apply reaction service by security intelligence
                Find the DFD using vulnerability templates
                if (True) then
                    Anomaly detection occur
                    Update the database using blockchain
                else
                    Forward the qi to provide service
                end
            end
        end
    end
end
```

mitigation of attack, respectively, for the smart home network.

Process flow. The flow of the security approach in the smart home network is initialized with algorithm 1 which provides service to the authenticated client. Initially algorithm 1 for the time period t_1 home gateway checks for the client authentication and then analyzes the query packet q_i whether the query is valid or not as per the data available in the database. The home gateway also checks for some packet, if it is an old query that means it is not a new flow in the network. It processes the request and responds to the client. Otherwise, if the packet query is a new flow, it will go for further analysis as per algorithm 2 for the detection and mitigation. Initially, for the time t_2, the new packet query q_i is forwarded to detection mechanism from where it checks whether the signature of the query packet is with known attack database. If the signature of query packet is matched with an already existed malicious packet signature, it immediately discards and notifies the home controller. Otherwise, it extracts the feature qi for the traffic using Triangle Area Map (TAM) of MCA[25]. And then check anomaly pattern pi of qi analyzed by MCA detection methods to get the correlation features among the traffic.

When there is any anomaly or infected packets enter into the home network, an alert is generated with updating notification to the home gateway and the packet is forwarded to the further analysis in the intelligence security analysis. The intelligence system finds the data-flow diagram (DFD) and gets the vulnerability from vulnerability templates. If the vulnerability is detected, it discards the packet, updates the rule, stores the pattern in the block as a transaction of the node, and informs to the known attack database using blockchain technology. If there is no vulnerability found, it will simply forward the packet to the home network.

The home network protects potential Internet-based attackers through NAT services. However, client devices can exploit the Universal Plug-n-Play (UPnP) port forwarding feature in typical home gateways, exposing them to Internet attacks. Though protocol-specific traffic is characterized by known packet header, we apply the rules in the home controller to capture the traffic and forward to the detection and analysis engine. The rules ensure normal forwarding of the traffic and sending a mirror copy to the analysis engine. This allows the home controller to provide data plane forwarding affected by intrusion detection process. The MCA is applied to traffic in which the basic feature generation for individual records is divided into two categories based on raw or original features and normal. In MCA analysis, the triangle area map generation is applied to extract the correlation between distinct features from traffic records. Triangle area map stored all the extracted correlations which are then used to replace the normalized features. This helps to distinguish the legitimate and the anomaly traffic records.

DoS attacks traffic works on valid network traffic, and the behavior of network traffic is responded by the statistical nature of the detection system. To illustrate this statistical nature, this module presents the MCA approach in the DoS attack detection module. Here, the MCA employs the triangle area to improve correlation information between features in the observed data objects in the system.

Profile generation. In this module, a normal profile presents a threshold-based anomaly detector generated using purely valid network traffic records and uses it to compare against new incoming traffic survey records. By applying the proposed triangular area-based MCA approach initially, we analyze the valid network traffic and use the generated TAM to obtain the most unique properties for generic profile generation in the system. In this module, a normal profile presents a threshold-based anomaly detector generated using purely valid network traffic records and uses it to compare against new incoming traffic survey records. By applying the proposed triangular area-based MCA approach initially, we analyze the valid network traffic and use the

generated TAM to obtain the most unique properties for generic profile generation in the system.

In the detection mechanism, it is an intelligent security model which essentially cooperates and utilizes the latest knowledge base. It is a collaboration scheme of the following three security services. Protection services are designed to reduce attacks.

Detection service receives activity data from smart home applications, devices, and networks; analyzes captured home network data; and finally detects anomalies. With the help of the defense mechanism, the reaction service helps the smart home to survive all attacks. These security services are designed using dynamic algorithms, and currently, there is a strong linkage between these services to defend against possible and invisible attacks. When an intrusion is detected, the discovery service orders the response service and minimizes further attacks by sharing the discovery detection experience with the protected service. The response service responds to action commands from the detection service to eliminate the risk of system malfunction and share the behavioral experience with detection and protection services. These reaction services are designed using dynamic algorithm and they have strong linkage between these services against possible attacks. The reaction services also mitigate the vulnerability by analyzing data flow diagram. In addition, Active Security System (ASSYST) is designed to provide a mechanism to respond to DDoS attacks. This is a router-level architecture, whose components are internal to the network router and have nothing to do with end systems. The system is powered by the output from an external intrusion detection system (IDS) that performs real-time traffic analysis, with the goal of detecting potential attack attempts.

Attack detection. This section describes a threshold-based anomaly detector that is used to generate regular profiles using legitimate network traffic records and compare them with future newly received survey traffic records. The difference between new incoming traffic records and each regular profile is checked by the proposed detector. If the dissimilarity is greater than the predetermined threshold, the traffic record is flagged as an attack. Otherwise, it is displayed as a legitimate traffic record. Obviously, the normal profiles and thresholds directly influence the performance of the detector based on the threshold. Low-quality regular profiles cause erroneous characterization of legitimate network traffic. Thus, we applied the proposed triangulation area-based MCA method first, analyzed legitimate network traffic, and used high-quality features for normal profile generation using the generated TAM provide.

The normal profile generation for l number of legitimate traffic record $\mathrm{R}^{\mathrm{normal}} = \{r_1^{normal}, r_2^{normal} \ldots\ldots\ldots r_l^{normal}\}$ is analyzed by MCA approach by TAM generation. The number of legitimate traffic in lower part of TAM in the traffic is

$$R_{TAM_{lower}}^{normal} = \left\{TAM_{lower}^{normal,1}, TAM_{lower}^{normal,2}, \ldots TAM_{lower}^{normal,l}\right\}$$

The Mahalanobis Distance (MD) is used to measure the traffic records, and to differentiate the traffic records from legitimate traffic, a threshold selection is required and defined as $Threshold = \mu + \sigma \times n$. For normal distribution n is ranged from 1 to 3.[33] This means that we would like to determine the detection with a certain degree of confidence in the range 68% to 99.7% associated with the selection of various values of n. Therefore, if the observed MD is greater than the threshold, it is considered an attack.

Security and privacy analysis. As for as the smart home concerns, security is very important issue to deal with it. Introducing the blockchain in the smart home network at very large scale brings a lot of security advantages.

Fulfilling security requirement for IoT smart home: For the IoT smart home blockchain comes with great data protection capabilities. Having immutable decentralized ledger technology is used for monitoring as well as copying backup of transactions between connected devices in the smart home networks. The integrity and confidentiality come from seamless message exchange transaction through smart contracts. In addition, service quality and authenticity are two important concerns for all customers. Because these smart contract act as agreements between communication devices which do not required intermediates. It ensures end-to-end privacy policy.

The third important security parameter is availability of services in smart home network. Blockchain provides the availability in terms of responsiveness by defining the notion of transaction commit needed by running applications. To increase the availability in the smart home, there should be protection service against malicious attack. One way to resolve the issue is by limiting the transaction of those objects which has already established the shared key. Transaction received from the overlay network is authorized by minors. In addition, MCA detection approach in the proposed algorithm will help to mitigate the DDoS attack by identifying the malicious packets and provide the resource available to the smart home running application.

Traceability of transaction: Blockchain provides a digital record where no one can change it rather confirmation from sender receiver and miners. This is the big advantage of introducing blockchain in smart home network where for each transaction, user login are

saved and records. It also protects from the insider threat and notifies the miners immediately.

Evidence basis blockchain: Blockchain will help in the field of cyber forensics by providing the evidence based as all activities are recorded and stored in the ledger. Companies can compete against fraud, financial crime, and digital rights theft. Defining all logs is one of the main goals of cyber forensic experts and keeping track of all activities (and its time) created by network participants.

Minimizing human error in smart home: Preparing the documents on paper for smart homes will be vulnerable for security reason such as data theft, loss of important documents, and data changes. The company that provides the smart home should manage very strong password and manage very strong security to manage and protect it. This will become more costly in terms of overall budget of smart home. Therefore, blockchain will provide a good solution with great data protection by providing and deploying encrypted identity Secure Sockets Layer (SSL) certificate and hash function included and verified on distributed ledger.

Mitigating DDoS attack: As growing the smart homes and built large size IoT network, the adversaries are more attracted to deploy the DDoS attack on it. Our proposed architecture protects against DDoS attack using its hierarchical and MCA detection approach. All the transaction is monitored and verified by miners, and it is very difficult and impossible to compromise them. Whether the IoT device of smart home is compromised by attackers will be analyzed by MCA approach.

Experimental analysis

Detailed performance evaluation of the proposed architecture was performed in various scenarios. We performed the identification accuracy test of attack detection model using network traffic. The security model analyzes the anomaly detection in the smart home network. This section shows the results of the evaluation. In addition, we evaluate performance evaluation using blockchain technology in the smart home tier and overlay for their independent operation.

Experimental setup

For the implementation of the proposed system, ZigBee technology is used which is based on IEEE 802.15.4 standard. The Ad Hoc communication varying range of smart home is approximate 15 × 21 sq.m. The data rate is 200 kbps with large-scale low power configuration. These features make ZigBee the ideal communication technology in smart home networks. The simulation parameters are as shown in Table 1.

Table 1. Simulation parameters.

Parameters	Values
Network simulator	Netsim
No. of the nodes	20
Simulation time	100 s
Data rate	200 kbps
Network area	15 × 21 sq.m.
Size of the packet	512 bytes

Table 2. Comparison of performance metrics.

	Average FPR	Average TPR	+ ve likelihood	–ve likelihood
TRW-CB	.50	.80	1.6	.40
NetAD	.50	.78	1.56	.44
MaxEnt	.50	.82	1.64	.36
SH-BlockCC	.50	.89	1.78	.22

FPR: False Positive Ratio; TPR: True Positive Ratio.

Evaluation data set

We used the CASAS dataset[34] to evaluate attack detection capability. CASAS datasets are smart home-based data sets. It is a research project by Washington State University (WSU). The CASAS project treats the environment as an intelligent agent. The environment where the controller is used that address the status of the occupant and its surroundings. These are recognized using sensors that enhances the comfort, safety, and productivity of the occupant.[35,36] In the smart home, various kinds of sensors are used which are located in a different location within the smart home such as sensor door, refrigerator sensor, boiler sensor, the sensor in the kitchen area. By testing this dataset approach, it has become possible to contribute attractive evaluation and compare with other methods. Zero percent of the labeled data is being used by evaluation process which includes legitimate traffic and smart home–specific protocol traffic.

Performance evaluation of security parameters in smart home network

TPR (True Positive Ratio) and FPR (False Positive Ratio) are the performances metrics to determine the accuracy of the proposed model. Positive likelihood and negative likelihood are metrics measured by the ratio of TPR with FPR (False negative Ratio) and FNR to TNR (True negative Ratio), respectively. The SH-BlockCC gives better result as compared with TRW-CB, NetAD, and MaxEnt (Table 2).[36]

As shown in Figure 6, the throughput of our proposed model is approximately 75 Mbps maximum. In

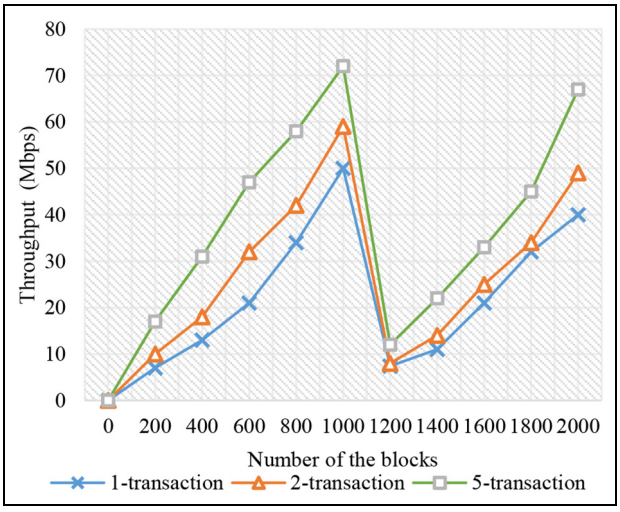

Figure 6. Throughput of the system.

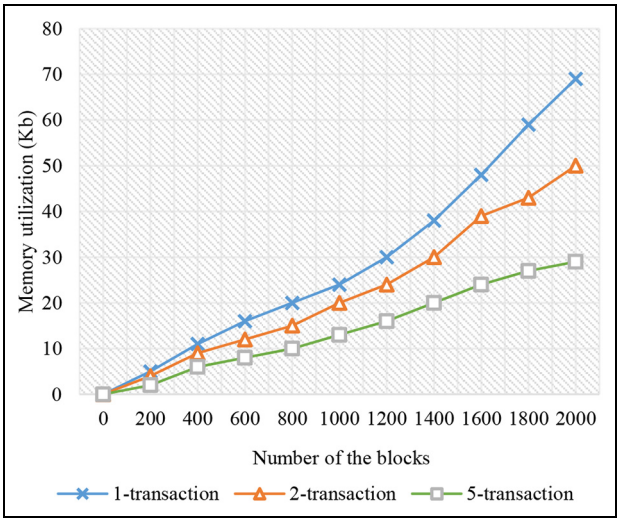

Figure 7. Memory utilization of the system.

the normal case, as the number of blocks increases, and for increased transaction, the throughput increases. At the time of t where number of blocks are 1000, there is a flooding attack in the network, the throughput of the system immediately decreases because of too much congestion and processing of packets in the network. After some duration of time, it becomes uniform to some extent and then gradually increases and recovers at a certain level.

Performance evaluation using blockchain technology

Here, we evaluate the various performance aspects of the proposed model. We separately evaluate the smart home tier and overlay for their independent operation. Here we use two simulators as follows:

Cooja: It is built over Contiki OS which is optimized to be little memory and minimal processing capabilities. Cooja is well suited for resource-constrained IoT devices. It emulates various functions of IoT devices such as lighting, heating, and pressure.[37]
Netsim: It is a simulator and emulator to test IoT networks and applications. Here we used it to evaluate the overlay performance.

Blockchain-based proposed model experiences computational overhead and time overhead on the smart home device. To evaluate this, we conduct simulation using Cooja and Netsim for local block manager device to get time and energy consumption, since the local block manager processes all the transactions and performs both symmetric and asymmetric encryption. Amazon EC2 cloud data center is directly connected to miners to store the data. Here, we evaluate the store and access simulations. A low resource constrains communication protocol is used for smart home setting. Four Z1 mote sensors are used for simulation which periodically sends the data to the miner for every 5 s.

Memory utilization of the SH-BlockCC is shown in Figure 7. The figure shows the memory utilization for the different block size of one, two, and five transactions per block. As the transaction increases per block, the memory utilized can be reduced. If the number of blocks is increased due to the fixed transaction, more memory is occupied. The results shows higher memory is utilized for lower transaction and vice versa. If the transaction per block is increasing up to a limit where it meets the block size, then the new block will be automatically formed. However, the memory utilization increases with increasing the number of transactions per block. Therefore, more number of transactions per block will reduce memory utilization.

The execution time and network delay are shown in the Figures 8 and 9, respectively. The execution time is measure at the starting point where the block is created and processed. However, both execution time and network delay in millisecond (ms) are increasing as the number of blocks and transaction are increasing.

Network overhead in blockchain application is the traffic overhead occurred in the network. Here, we evaluate the network overhead by varying the number of nodes in consortium network. As shown in Figure 10, for the increased number of nodes, the network overhead is also increasing accordingly. It is happened due to the fact that the multiple transactions between nodes are increasing, establishing the consensus among nodes, and during miner selection process.

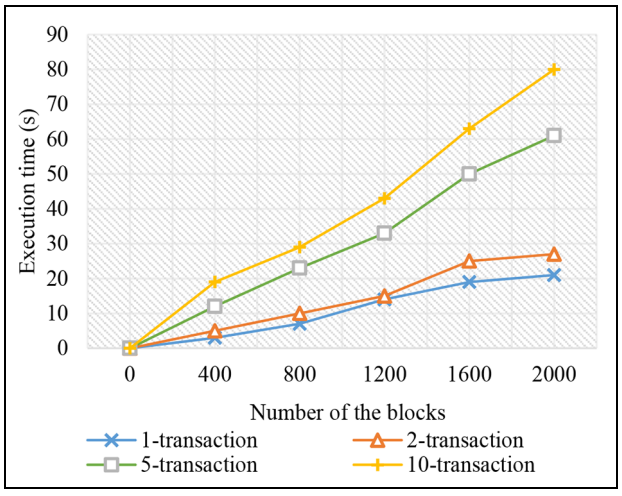

Figure 8. Execution time.

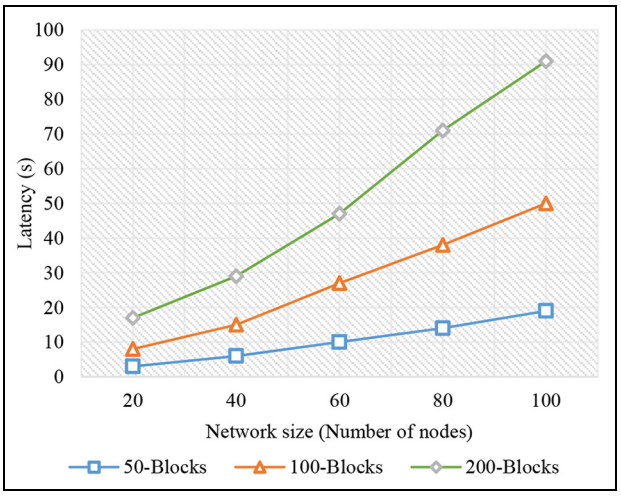

Figure 11. Latency (with Blocks).

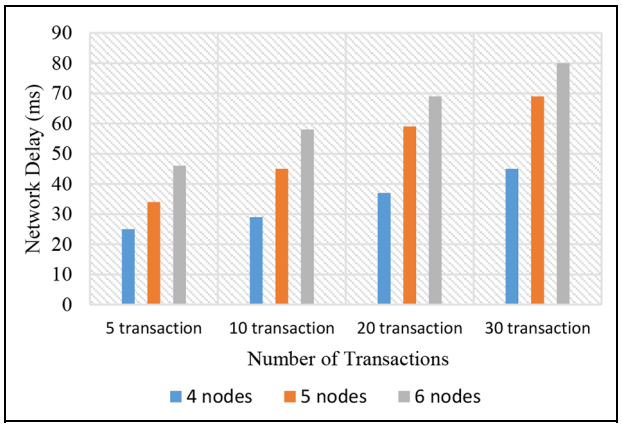

Figure 9. Network delay.

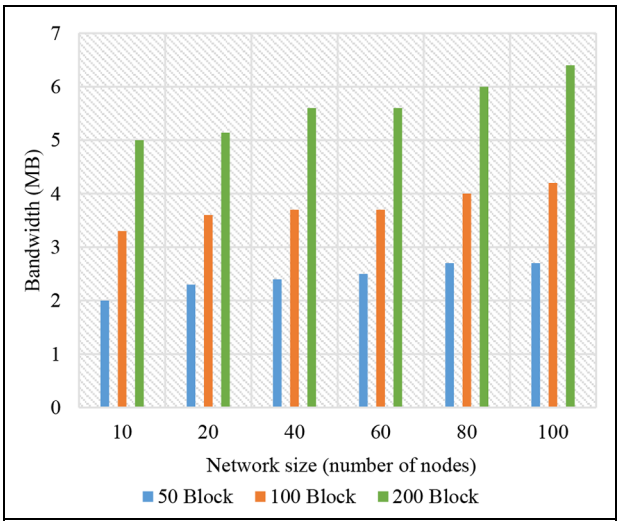

Figure 12. Bandwidth.

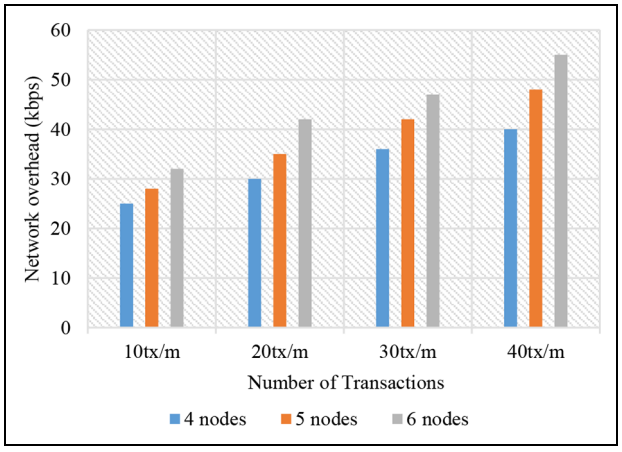

Figure 10. Network overhead.

Scaling the blockchain

To scale the blockchain, we took approximately 100 nodes. The metrics involved to measure the scalibility in the our simulation are letancy and bandwidth consumption per node. We increase the network size in terms of nodes commnicated. Figure 11 depicts the latency for different number of micro blocks. Initially, the latency rate is low as the less number of nodes are participating in the network. However, as the network size is growing, the latency rate is getting higher because of more processing time were consumed by the nodes. The bandwidth consumption of the network increases with increasing the network size and number of blocks as shown in Figure 12. It is because of broadcasting of all blocks to the networks.

Figures 13 and 14 are the comparisions of our proposed framework with core model of delay occurred and throughput, respectively. The proposed framework includes the blockchain concept to increase its performance; however, core model is pure cloud based that

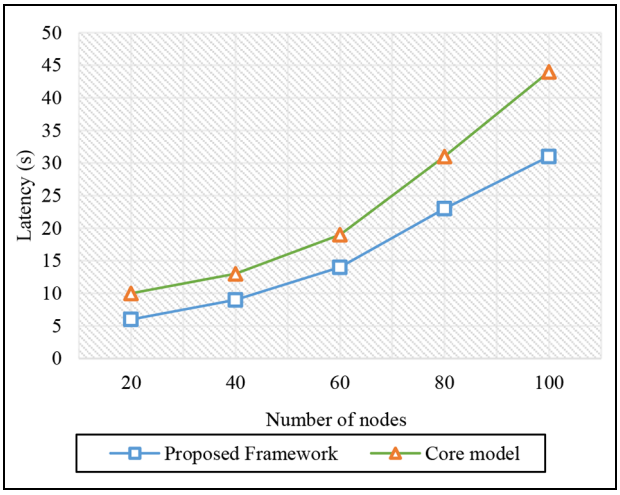

Figure 13. Overall Latency.

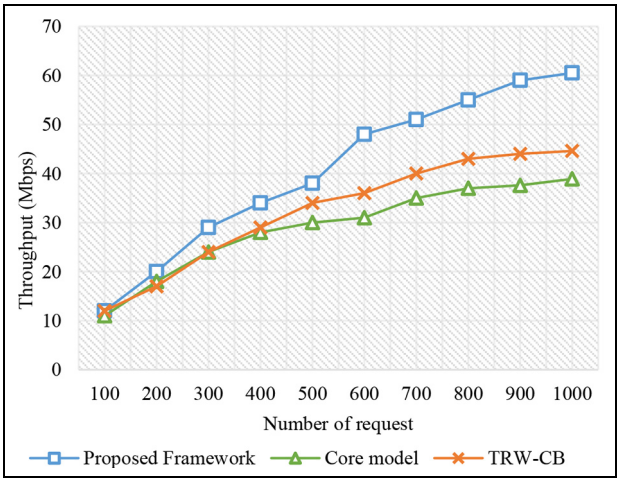

Figure 14. Throughput (Normal case).

does not uses the blockchian concept. The variation in the dealy associated with the number of nodes by the IoT devices shows an increase in delay as the number of nodes increases in the network. Compared to the core data center, there is less in delay than proposed model. We also compared the throughput in the normal scenerio where there is no attack occurred (Figure 13). The throughput of proposed model increases as the number of request increases by the IoT nodes. The output results in this figure provides higher throughput in proposed model compared with core infrastructure and TRW-CB. Whereas in attack case, the throughput shown in Figure 15, after some time of running the application at time t = 60 s, there is a flooding attack in the network, the throughput of the system rapidly decreases, but less decreasing than core model and TRW-CB. And it recovers fastly than other two up to a certain level. The proposed model recovers more fastly than other two method because of lack of proper

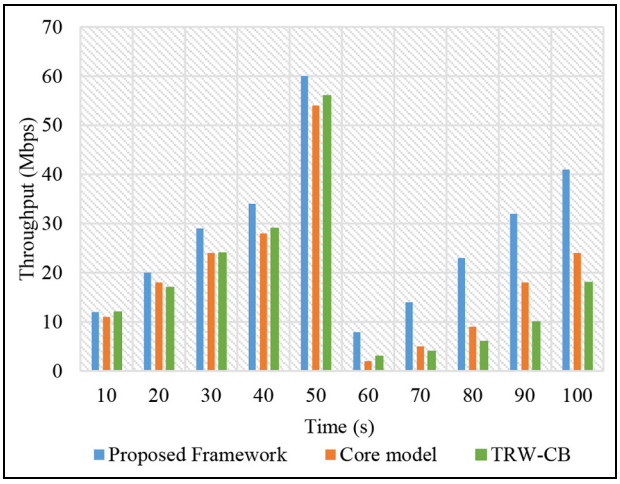

Figure 15. Throughput (Attack case).

methodology. On the other hand, the proposed model effectively handles the flooding attack by MCA algorithm and continuously checking the request by the validator in construim blockchian network. The unauthorized request transaction were denied after a certain unsuccessful number of request.

Comparision with existng researches and discussion

This section provides us the analysis of our proposed work compared with the existing works. The comparison analysis is based on security parameters confidentiality, authentication, availability, integrity, and privacy.

Acs and Castelluccia[38] proposed a scheme for privacy preserving of smart meter in smart home by utilizing homomorphic encryption. The algorithm provides the confidential and privacy of smart meter.

The integrity of message and authentication are achieved by Mantoro et al.[39] This research is about defense mechanism using smart phone. The scheme utilizes Diffie-Hellman and RC4-based hash functions to secure authentication and assure integrity of message communicated between devices. Lee et al.[40] proposed a frequency Quorum Rendezvous (FQR) that exploits a random spectrum-based wireless communication for protecting against powerful attacks. IDS are deployed against DoS attack.

Moosavi et al.[41] proposed a secure architecture based on Datagram Transport Layer Security (DTLS) handshake protocol. This work focuses on authentication and authorization for IoT devices. It uses a more secure key management scheme between sensor nodes and the smart gateway. Furthermore, the impact of DoS attacks is reduced due to the distributed nature of the architecture.

A secure IoT-based smart home automation system was developed by Pirbhulal et al.[42] To facilitate energy-

Table 3. Comparison analysis of existing researches with proposed solution.

	38	39	40	41	42	SH-BlockCC
Confidentiality	✓					✓
Authentication		✓		✓	✓	✓
Integrity		✓			✓	✓
Availability			✓	✓	✓	✓
Privacy	✓				✓	✓

efficient data encryption, a method namely Triangle Based Security Algorithm (TBSA) based on efficient key generation mechanism was proposed. The developed IoT-based system fulfills the security requirements.

Table 3 shows that SH-BlockCC covers all security parameters compare with the existing work. Therefore, the model SH-BlockCC fulfills the security requirements of the smart home network.

Conclusions

The article presented an efficient and secure smart home architecture based on cloud computing and blockchain technology. Cloud computing extended the domain of smart-home to get benefit from cloud providers to the users. The efficient broker managed the selection of energy-efficient service providers to the end users and blockchain technology provides a peer-to-peer network where non-trustable nodes are communicating to efficient processing network. We used encryption and hashing algorithm in blockchain technology to achieve confidentiality and integrity in a local smart home network and an overlay network. Authorization is achieved by policy header and shared key between device and miners, and availability is achieved by acceptable transactions between devices and miners. In addition, we also discussed MCA detection algorithm that is applied to the smart home network for identifying the correlation between traffic features. Overall, the proposed architecture provides a network attack detection and response system at smart homes. According to our results in terms of receiver operating characteristic (ROC) curve, CPU utilization, throughput time overhead, and network overhead, our proposed architecture can make the smart home more secure and efficient.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2015-0-00378) supervised by the IITP (Institute for Information & communications Technology Promotion) and supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2018-0-00508, Development of blockchain-based embedded devices and platform for MG security and operational efficiency).

ORCID iDs

Saurabh Singh https://orcid.org/0000-0003-1118-9569
Weizhi Meng https://orcid.org/0000-0003-4384-5786

References

1. Ahvar E, Daneshgar-Moghaddam N, Ortiz AM, et al. On analyzing user location discovery methods in smart homes: a taxonomy and survey. *J Netw Comput Appl* 2016; 76: 75–86.
2. Lutolf R. Smart home concept and the integration of energy meters into a home based system. In: *Proceedings of the seventh international conference on metering apparatus and tariffs for electricity supply*, Glasgow, 17–19 November 1992. New York: IEEE.
3. Ke X, Xiaoliang W, Wei W, et al. Toward software defined smart home. *IEEE Commun Mag* 2016; 54: 116–122.
4. Smart home seamless life unlocking a culture of convenience, 2017, https://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-consumer-intelligence-series-iot-connected-home.pdf
5. Shin D, Sharma V, Kim J, et al. Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access* 2017; 5: 11100–11117.
6. Houbing S, Danda R, Sabina J, et al. *Cyber-physical systems: foundations, principles and applications*. Boston, MA: Academic Press, 2016.
7. Pishva D and Takeda K. Product-based security model for smart home appliances. *IEEE Aerospace Electron Syst Mag* 2008; 23(10): 32–41.
8. Singh S, Sharma PK and Park JH. SH-SecNet: an enhanced secure network architecture for the diagnosis of security threats in a smart home. *Sustainability* 2017; 9: 513–532.
9. Sharma V, You I and Kul G. Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain. In: *Proceedings of the 2017 international workshop on managing insider security threats*, Dallas, TX, 30 October 2017, pp.81–84. New York: ACM.
10. He Q, Xu Y, Liu Z, et al. A privacy-preserving Internet of things device management scheme based on blockchain. *Int J Distrib Sens N* 2018; 14: 1–12.
11. Jacobsson A and Davidsson P. Towards a model of privacy and security for smart homes. In: *Proceeding of 2015 IEEE 2nd world forum on Internet of things (WF-IoT)*,

Milan, 14–16 December 2015, pp.727–732. New York: IEEE.
12. Dorri A, Kanhere SS and Jurdak R. Blockchain in Internet of things: challenges and solutions, arXiv:1608.05187.
13. Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems. *Future Gener Comput Syst*, https://arXiv.org/abs/1802.06993
14. Singh S, Jeong YS and Park JH. A survey on cloud computing security: issues, threats, and solutions. *J Netw Comput Appl* 2016; 75: 200–222.
15. Singh S, Sharma PK, Moon SY, et al. EH-GC: an efficient and secure architecture of energy harvesting green cloud infrastructure. *Sustainability* 2017; 9: 673–691.
16. Hegade R and Patil V. Green cloud computing. *Int J Eng Adv Technol* 2015; 4: 1–4.
17. Balasooriya PN, Wibowo S and Wells M. Green cloud computing and economics of the cloud: moving towards sustainable future. *GSTF J Comput* 2016; 5: 15–20.
18. Jadhav NY. *Green and smart building trends*. Singapore: Springer, 2016, pp.9–14.
19. Chaqfeh MA and Mohamed N. Challenges in middleware solutions for the Internet of things. In: *Proceeding of 2012 international conference on collaboration technologies and systems (CTS)*, Denver, CO, 21–25 May 2012, pp.21–26. New York: IEEE.
20. Lu C. Overview of security and privacy issues in the Internet of things, 2014, https://www.semanticscholar.org/paper/Overview-of-Security-and-Privacy-Issues-in-the-of-lu/51a2f7f44be58260b25c40834ec28050bacfbddf
21. Mendez DM, Papapanagiotou I and Yang B. Internet of things: survey on security and privacy. arXiv:1707.01879.
22. Byun J, Jeon B, Noh J, et al. An intelligent self-adjusting sensor for smart home services based on ZigBee communications. *IEEE T Consum Electr* 2012; 58: 794–802.
23. Jing Z, Laurence TY, Man L, et al. A survey: cyber-physical-social systems and their system-level design methodology. *Future Gener Comput Syst* 2016; 2016: 1–15.
24. Eric KW, Yunming Y, Xiaofei X, et al. Security issues and challenges for cyber physical system. In: *Proceedings of 2010 IEEE/ACM Int'l conference on green computing and communications and international conference on cyber, physical, and social computing*, Hangzhou, China, 18–20 December 2010, pp.733–738. New York: IEEE.
25. Tan Z, Jamdagni A, He X, et al. A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE T Parallel Distrib Syst* 2014; 25: 447–456.
26. Houbing S, Glenn AF and Sabina J. *Security and privacy in cyber-physical systems: foundations, principles and applications*. Chichester: Wiley-IEEE Press, 2017, pp.1–472.
27. Houbing S, Ravi S, Tamim S, et al. *Smart cities: foundations, principles and applications*. Hoboken, NJ: John Wiley & Sons, 2017, pp.1–906.
28. Amadeo M, Molinaro A, Paratore SY, et al. A cloud of things framework for smart home services based on information centric networking. In: *Proceedings of IEEE 14th international conference on networking, sensing and control (ICNSC)*, Calabria, 16–18 May 2017. New York: IEEE, pp.245–250.
29. Stojkoska BLR and Trivodaliev KV. A review of Internet of things for smart home: challenges and solutions. *J Clean Prod* 2017; 140: 1454–1464.
30. Yunchuan S, Houbing S, Antonio J, et al. Internet of things and big data analytics for smart and connected communities. *IEEE Access* 2016; 4: 766–773.
31. Abbasi AA and Younis M. A survey on clustering algorithms for wireless sensor networks. *Comput Commun* 2007; 30: 2826–2841.
32. Dorri A, Steger M, Kanhere SS, et al. Blockchain: a distributed solution to automotive security and privacy. *IEEE Commun Mag* 2017; 55: 119–125.
33. Tan Z, Jamdagni A, He X, et al. Denial-of-service attack detection based on multivariate correlation analysis. In: *Proceeding of international conference on neural information processing*, Shanghai, China, 13–17 November 2011, pp.756–765. New York: Springer.
34. Cook D. CASAS smart home project, 2017, http://www.ailab.wsu.edu/casas/
35. Synnott J, Nugent C and Jeffers P. Simulation of smart home activity datasets. *Sensors* 2015; 15: 14162–14179.
36. Mehdi SA, Khalid J and Khayam SA. Revisiting traffic anomaly detection using software defined networking. In: *Proceeding of international workshop on recent advances in intrusion detection*, Menlo Park, CA, 20–21 September 2011, pp.161–180. New York: Springer.
37. An Introduction to Cooja, 2016, https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja
38. Acs G and Castelluccia C. Dream: differentially private smart metering. *arXiv*:1201.2531.
39. Mantoro T, Ayu MA and Binti Mahmod SM. Securing the authentication and message integrity for Smart Home using smart phone. In: *Proceeding of 2014 international conference on multimedia computing and systems (ICMCS)*, Marrakech, Morocco, 14–16 April 2014, pp.985–989. Piscataway, NJ: IEEE
40. Lee E, Oh SY and Gerla M. Frequency quorum rendezvous for fast and resilient key establishment under jamming attack. *ACM SIGMOBILE Mob Comput Commun Rev* 2011; 14: 1–3.
41. Moosavi SR, Gia TN, Rahmani AM, et al. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput Sci* 2015; 52: 452–459.
42. Pirbhulal S, Zhang H, Alahi ME, et al. A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors* 2016; 17: 69–88.